IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF INFORMATION FROM GOOGLE ACCOUNTS:

TD102322@GMAIL.COM

THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.

FILED UNDER SEAL

Case No. 3:21sw103

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christopher M. Page, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of information that is stored at premises regarding Google Account TD102322@GMAIL.COM ("SUBJECT ACCOUNT") controlled by Google LLC (Google), a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations ("HSI") within the Immigration and Customs Enforcement ("ICE") Department of Homeland Security ("DHS") and has been so employed since December 2019. As a Special Agent with HSII, I am authorized to investigate crimes involving violations of federal law, to include: 21 U.S.C. Chapter 13, and 18

U.S.C. Prior to becoming an HSI Special Agent, I was employed as a State Trooper with the Virginia State Police for eight years. During my time as a State Trooper, I was trained to investigate many types of violations of state law to include motor vehicle and criminal statutes. I spent six years as a State Trooper assigned to the Counter-Terrorism and Criminal Interdiction Unit (CCI) as a narcotics detection canine handler. While assigned to CCI, I investigated numerous incidents of narcotics and currency smuggling as well as other types of interstate smuggling. Prior to being employed as a State Trooper, I was employed for one year as a Correctional Officer with the Virginia Department of Corrections. In 2009, I received a Bachelor of Arts degree in Criminal Justice from The Citadel, The Military College of South Carolina, located in Charleston, South Carolina.

3. I am a graduate of the Federal Law Enforcement Training Center (FLETC) located in Glynco, Georgia. At FLETC, I was trained in, among other things, criminal investigative techniques, narcotics smuggling, and money laundering investigations. While working for HSI, I have conducted and participated in investigations of violations of federal law, to include the trafficking of illicit narcotics and subsequent laundering of the proceeds. I am authorized to investigate and make arrests involving violations of federal law, including drug trafficking, and to execute warrants issued under the authority of the United States.

4. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other sworn law enforcement officers. This affidavit is intended to show that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge about this matter.

RELEVANT STATUTORY PROVISIONS

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 841(a)(1), Possession with Intent to Distribute a Controlled Substance, and 18 U.S.C. § 1956, Laundering of Monetary Instruments, have been committed by Johana MERCADO, Thomas Duong, and others, both known and unknown, in furtherance of drug distribution within the Eastern District of Virginia. There is also probable cause to search the information as described in Attachment A for evidence of these crimes as described in Attachment B, incorporated herein by reference.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated as defined by 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. The following paragraphs are all known based on my training and experience.

8. Cellular devices, such as mobile telephones, are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. To send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called "cell sites," which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, but the service area of a given cell site will depend on many factors, including the distance between towers. As a result, information about what cell site a cellular device connected to at a

specific time can provide the basis for an inference about the general geographic location of the device at that point.

9. Many cellular devices such as mobile telephones have the capability to connect to wireless internet ("Wi-Fi") access points if a user enables Wi-Fi connectivity. Wi-Fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a Service Set Identifier ("SSID") that functions as the name of the Wi-Fi network. In general, devices with Wi-Fi capability routinely scan their environment to determine what Wi-Fi access points are within range and will display the names of networks within range under the device's Wi-Fi settings.

10. Many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices; for example, a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices. That device emits beacons which can be detected by mobile devices within the Bluetooth device's transmission range to which it might connect.

11. Many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographic coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

12. Google is a company that offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android OS has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

13. Google offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google), online file storage (including Google Drive, Google Photos, and YouTube), messaging (Google Hangouts, Google Messages, and Google Chat), and video calling (Google Duo). Some services—such as Gmail, online file storage, and messaging—require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and YouTube, can be used while signed into a Google account, although some aspects of these services can be used even without being signed into a Google account.

14. Google offers an internet browser ("Chrome") that can be used on both computers and mobile devices. A user has the ability to sign in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browser. However, Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on many devices, including Apple devices.

15. In the context of mobile devices, Google's cloud-based services can be accessed either via the device's internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

16. Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes such as tailoring search results based on the user's location,

determining the user's location when Google Maps is used, and providing location-based advertising. Google also collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Regardless of the device, Google typically associates the collected location information with the Google account on the Android device and/or that Google account signed in via the relevant Google application. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about Wi-Fi access points and Bluetooth beacons within range of the mobile device.

17. Google collects and retains information about the user's location if the user has allowed Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol (IP) address at the time they engage in certain internet and app-based activity. Google associates this information with the Google account associated with the Android device and/or that Google account signed in with the relevant Google application.

18. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. Google has the ability to determine whether devices with particular Google accounts logged into them were in a specific geographic area at a specific time based on location data collected via the use of Google products as described above. Among other things, this information can inculpate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

19. When individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses,

and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

20. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

21. When users link their devices to their Google accounts, the names, addresses, phone numbers, email addresses, notes, and pictures associated with them are transferred to the phone and vice versa. This process is continually updated so when a contact is added, deleted, or modified using either the Google account or the mobile device, the other is simultaneously updated. This information is pertinent to the investigation as it will assist with identifying previously unknown co-conspirators and/or witnesses.

22. Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent

from other users, or uploaded from a user's mobile device. In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. A review of these images would provide evidence depicting the suspect, their associates, and others performing incriminating acts. These image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation.

23. Google operates an online app store whereby Google and other third-party vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can communicate outside a mobile device through the internet. These various applications facilitate communication using voice over internet protocol (VOIP) technology, short message system (SMS) text messages, multi-media messaging system (MMS) text messages, audio transmissions of recorded messages, and recorded or live video messages. As these services often operate independently of the mobile OS, there may be no communication information with the OS provider (i.e., Google does not store information in the Twitter app). Identifying communication applications purchased, downloaded, and/or installed on the mobile device would assist the investigators by determining which application provider should be served with additional search warrants. Furthermore, identifying the user's applications would assist investigators with determining banking and/or other financial institution information and social media sites used. Identifying the purchased or installed applications could identify apps that appear to the observer to be a calculator or other innocuous-appearing program. In reality, however, the applications are used to conceal pictures, videos, or other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices, as existing technologies are not designed to detect and locate them and the information they conceal.

PROBABLE CAUSE

24. In December of 2020, Homeland Security Investigations (HSI) initiated an investigation into the drug trafficking activities of Thomas DUONG, and other members of the DUONG Drug Trafficking Organization (DTO), based on information gathered from several investigations/seizures that were being conducted independently by Chesterfield County Police Department (CCPD) in Chesterfield, Virginia, and other HSI offices across the United States.

25. In September of 2020, Customs and Border Protection (CBP) officers at the San Ysidro, CA Port of Entry (POE) inspected a vehicle—a black, 2016 Range Rover—in the southbound lanes. The occupants of the vehicle, Johana MERCADO and Eric GARCIA, provided inconsistent information to CBP officers about the reason for their trip and the declaration of any currency. During a secondary inspection, officers discovered $19,381 on the occupants' persons and in the vehicle. CBP also conducted an extraction of MERCADO's cell phone. In the report, text messages and photos were obtained that revealed a larger organization and some of the inner workings of that organization, but the extraction yielded only limited information.

26. Text messages from the extraction identify an individual named "TD" or "T". Text messages between MERCADO and TD referenced setting up travel arrangements, paying couriers, and smuggling U.S. Currency and marijuana. The contact information for TD had a phone number as well as a picture of an Asian male. Upon investigation the phone number and photo were found to belong to Thomas DUONG.

27. The extraction also revealed more text messages to an individual identified as Nicole Andrei CLEMENTE. In text messages between MERCADO and CLEMENTE, MERCADO told CLEMENTE that CLEMENTE could make $2,000 per trip by moving two suitcases of vacuum-sealed marijuana to Virginia and North Carolina and bringing U.S. Currency

back to California. MERCADO told CLEMENTE that CLEMENTE would check two suitcases containing marijuana for CLEMENTE's flight. Once CLEMENTE arrived at her destination, she would check into a hotel room. Once in the hotel room, DUONG would contact CLEMENTE and another individual would then pick the suitcases up from CLEMENTE. CLEMENTE would then receive another suitcase with the currency and CLEMENTE would count the currency. MERCADO then told CLEMENTE that CLEMENTE should hide the currency inside pairs of pants in the suitcases and stick a pillow and towel in the suitcase to keep the pants from moving around.

28. Search history from MERCADO's phone revealed the following:

- November 5, 2019: a search for flights from John Wayne Airport (SNA, in Orange County, California) to John Glenn Columbus International Airport (CMH);
- November 9, 2019: a search for flights from SNA to Norfolk International Airport (ORF);
- December 5, 2019: a search for flights to Greenville-Spartanburg International Airport (GSP) in South Carolina;
- September 13, 2020: two searches for flights from SNA to GSP;
- September 15, 2020: four searches for flights from SNA to GSP;
- September 16, 2020: four searches asking if North Carolina and South Carolina have the same time zone, and;
- September 16, 2020: four searches were conducted for hotels in Greenville, SC.

29. In the notes section of MERCADO's phone were notes listing prices for ticket/insurance, bags, taxi, hotel, and parking costs. A note dated August 17, 2020 and titled "NC" listed prices for the above-mentioned items. Subpoena records show that on August 24,

2020 MERCADO flew to Piedmont Triad International Airport (GSO) in Greensboro, NC and returned on August 26, 2020. A note dated September 3, 2020, titled "VA," lists prices for the above-mentioned items. Subpoena records show MERCADO flew to Richmond International Airport (RIC) on August 30, 2020 and returned on September 2, 2020.

30. In January 2021, HSI met with CCPD who had an open case on the local DTO in Chesterfield County, VA. CCPD subsequently provided HSI with a list of approximately eighteen identified couriers. These couriers were identified as belonging to the same DTO based on phone records, flight records, and social media information.

31. On January 22, 2021, a HSI Dallas Task Force Officer seized $92,040 vacuum sealed in two suitcases from an individual identified as Samira GARCIA-SALAZAR. GARCIA-SALAZAR's originating flight was Greensboro/High Point, NC with a connecting flight in Dallas and a final destination of Santa Ana/Orange County, CA. GARCIA-SALAZAR crossed the San Ysidro POE with MERCADO on February 10, 2021 in a vehicle registered to Jose NAVA, an identified courier.

32. On March 22, 2021, CCPD executed a state search warrant on MERCADO's checked bag in Richmond, VA. During the execution, CCPD located and seized $90,000 from MERCADO's checked bag. The currency was vacuum sealed and located in pants pockets exactly as described in text messages seen from the cell phone extraction performed by CBP.

33. On April 12, 2021, HSI and CCPD went to Fairfield Inn and Suites by Marriott Richmond Airport located at 5252 Airport Square Lane, Sandston, VA 23150. Based on cell phone pings, MERCADO was believed to have stayed at the hotel from April 7, 2021 through April 10, 2021, and DUONG stayed from April 8, 2021 through April 10, 2021. During review of video footage MERCADO was seen entering the hotel with two large suitcases and entering an

assigned hotel room. MERCADO was then seen exiting the hotel room and exiting the hotel via a side entrance to meet Korey LEWIS, a target of the CCPD investigation. MERCADO and LEWIS placed the two suitcases in LEWIS' vehicle and MERCADO reentered the hotel room. Later, MERCADO met with LEWIS and took possession of one suitcase. MERCADO and DUONG were seen checking out of the hotel at the same time on April 10, 2021. MERCADO was seen with only one suitcase, the same as the one obtained from LEWIS.

34. Subpoena returns show DUONG flew to Richmond, VA (RIC) from Santa Ana, CA (SNA) on April 8, 2021 through Chicago, IL (ORD). DUONG returned from Richmond, VA (RIC) to Santa Ana, CA (SNA) through Denver, CO (DEN) on April 10, 2021. DUONG used the email address TD102322@GMAIL.COM to book the flights.

35. Subpoena records link DUONG with flight reservations using the email address TD102322@gmail.com. TD102322@gmail.com was also documented in purported money service business data derived from multi-jurisdictional repositories of data approved for HSI use in interdicting and investigating the financial activities of complex national and international organized criminal elements/entities.

36. On April 14, 2021, HSI assisted CCPD with multiple search warrants on the local DTO. During the execution of the warrants, electronic devices were seized from LEWIS. A cell phone extraction was completed on LEWIS's cell phone and numerous SMS messages were obtained between LEWIS and DUONG. The messages lay out the operation starting with DUONG messaging LEWIS the name of the "runner," hotel address, and room number, and telling him to "Bring 1 luggage and wipe it down." DUONG then instructed LEWIS to bring a specific number of something, and what time the "runner" must leave to return. One message dated September 7, 2020, 9:52:48 PM read: "Courtyard by Marriott Richmond Airport, 5400

Williamsburg Rd, Sandston, VA 23150 Room 310 Bring both luggage and 110." Based on my training and experience, I believe the specific number to mean how much cash to bring. Further, I know that "runner" is a term for a courier or a person who transports an item. Additionally, based on SMS messages between MERCADO and CLEMENTE, I know that the operation is conducted with two pieces of luggage being dropped off to the local DTO with marijuana and one piece of luggage being returned to the "runner" with the U.S. Currency.

37. A "runner" by the name of Daniel CARTER was previously identified by CCPD and HSI as a member of the DUONG DTO. On April 14, 2021, CCPD provided information to HSI that CARTER was in Richmond, VA and had met with LEWIS. CARTER was believed to be staying at the Delta Hotels by Marriott Richmond Downtown located at 555 E. Canal St., Richmond, VA 23219. HSI went to the hotel and confirmed with hotel staff that CARTER was at the hotel and due to check out the same day. Hotel staff later contacted HSI and stated that CARTER had requested a late checkout of 2:00 p.m. CCPD provided HSI with information that CARTER never traveled back north to Ronald Reagan Washington National Airport (DCA) to return to California. Subpoena records later showed CARTER changed his reservation and flew from Richmond, VA (RIC) on April 15, 2021 back to California.

38. Location data from DUONG's phone placed DUONG at/near 14500 Hancock Village Street, Chesterfield, VA, which is the address for Longhorn Steakhouse. This information was corroborated by SMS messages sent between DUONG, THOMPSON, and LEWIS in a conversation asking for an address for dinner arrangements. It is then further corroborated with location data from THOMPSON and LEWIS' phones placing all the subjects in the same area at/around the same time and leaving the area at/around the same time. DUONG is observed on hotel video footage exiting a side door approximately the same time as DUONG's phone location

travels to Longhorn. DUONG is then observed later entering the hotel from the same side door approximately the same time as DUONG's phone location travels from Longhorn.

39. MMS messages were sent from DUONG to LEWIS with a ledger stating the following: the name of the "runner" with the date followed by a number circled indicating the number of pounds of marijuana being shipped, followed by the strain of marijuana, followed by the price per pound of each strain, and the product total circled at the bottom. From the conversation string between DUONG and LEWIS starting January 17, 2021 through April 14, 2021 there are a total of 66 MMS ledgers.

40. On April 3, 2021, at 8:15:13 PM, DUONG sent a SMS message to LEWIS asking, "Are u grabbing the load from Jaraset today." Based on other conversations between DUONG and LEWIS as well as information obtained from MERCADO's phone, "Jaraset" was identified as Jaraset GARCIA (J GARCIA). J GARCIA was identified through MERCADO's phone and CCPD's investigation as a "runner" for the DUONG DTO.

41. I conducted a search warrant on Google account JOHANAMERC@gmail.com (belonging to MERCADO) on May 17, 2021. Based on those returns, emails were obtained addressed to DUONG in MERCADO's inbox using MERCADO's Gmail address on multiple occasions. Records also show DUONG conducted two Venmo transactions to MERCADO with a memo of "rent" for a total amount of $1000.

42. On June 15, 2021, MERCADO and DUONG flew from Santa Ana, CA (SNA) to Baltimore, MD (BWI) through Dallas-Ft. Worth, TX (DFW) on the same flight with American Airlines. American Airlines website information showed MERCADO and DUONG sat in seats next to each other for the flights. On June 17, 2021, MERCADO and DUONG both changed their reservations and flew out of Ronald Reagan Washington National Airport (DCA) back to Santa

Ana, CA (SNA) through Dallas-Ft. Worth, TX (DFW). DUONG utilized the email address TD102322@GMAIL.COM to book his travel through American Airlines.

43. Electronic devices are one of the primary tools utilized by distributors of illegal narcotics to communicate. These communications occur between sources of supply, drug transporters, facilitators, and customers. These conversations include drug pricing, drug quantity, meeting locations, information about drug dealer's customers, associates, addresses, money drops, and sources of supply. These conversations take place through email, phone calls, text messages, multimedia messages, and numerous third-party applications. Electronic devices are capable of maintaining this data over months and years.

44. DUONG and MERCADO utilize electronic devices to communicate with members of the DTO and these devices are employed to conduct and set up illegal drug transactions.

45. I believe that the information held by Google, linked to DUONG's Google accounts, will contain information which will help identify DUONG's source of supply, other co-conspirators, and financial transactions related to money laundering. The information likely to be obtained from the data held by Google is relevant and material to the ongoing criminal investigation.

46. Based on the foregoing, I submit that there is probable cause to search information in the possession of Google relating to DUONG's Google account described in Attachment A during the time period described in Attachment A, as well as information that identifies the Google account with which those devices are associated, for evidence of the crime(s) at issue in this case.

CONCLUSION

47. Based on the foregoing, I respectfully request that the warrant sought herein

pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and 18 U.S.C. § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41. Because this information is stored at Google and may require searches in various time zones, the Government requests authority for this search to be conducted at any time, day or night.

Respectfully submitted,

Christopher M. Page
Christopher M. Page, HSI Special Agent

Reviewed and approved by AUSA Shea Gibbons

Subscribed and sworn to before me on July 19th, 2021, in Richmond, Virginia.

/s/ MRC
Honorable Mark R. Colombell, U.S. Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google and applies to the premises, described as:

I. Google Legal Investigations Support
Re: GMAIL
1600 Amphitheatre Parkway
Mountain View, California 94043

II. Located in the City of Mountain View, County of Santa Clara, and State of California

III. And the Google Account: TD102322@gmail.com

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google and to be seized:

(1) All data maintained by Google pertaining to the Gmail accounts identified as: TD102322@gmail.com, to include but not limited to contents of all the communications stored in the Gmail account, including emails stored in the inbox, starred, important, sent, drafts, trash, and notes folder to include photographic images/movies/videos. Including all records, files and contents of Gmail, Google Docs, Google Drive, Google Calendar, location history, Google Chrome Sync, Google Services, Google Maps engine, Google Photos, Google Profile and web history for the time period from January 1, 2019 through and including the present time.

(2) Account information, user name, account history, connected sites, search history, calendar information, contact information, wallet / checkout service information, installed application(s), device make(s), model(s), international mobile identification number (IMEI) or mobile equipment identifier number (MEID) of all associated devices linked to the Google account: TD102322@gmail.com, for the time period from January 1, 2019, through and including the present time.

(3) All records or other information regarding the identification of the account holder including name, address, telephone number(s), and any log in IP address used. All records of session time and durations, the date the account was created, the length of service, the account status, log files, and alternative email addresses linked or associated with the account(s) linked to Thomas DUONG and the above-mentioned

Gmail accounts, for the time period from January 1, 2019, through and including the present time.

(4) All records pertaining to communications with Gmail and any other person who has contacted Google regarding the account and actions taken, for the time period beginning January 1, 2019, through and including the present time.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC. and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC., and they were made by Google LLC. as a regular practice; and

b. Such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC. in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Google LLC. and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature